

Redacted Version of Trial Plan ISO Plaintiffs' Motion for Class Certification

BOIES SCHILLER FLEXNER LLP

David Boies (admitted pro hac vice)
333 Main Street
Armonk, NY 10504
Tel: (914) 749-8200
dboies@bsflfp.com

Mark C. Mao, CA Bar No. 236165
Beko Reblitz-Richardson, CA Bar No. 238027
Erika Nyborg-Burch, CA Bar No. 342125
44 Montgomery St., 41st Floor
San Francisco, CA 94104
Tel.: (415) 293-6800
mmao@bsflfp.com
brichardson@bsflfp.com
enyborg-burch@bsflfp.com

James Lee (admitted pro hac vice)
Rossana Baeza (admitted pro hac vice)
100 SE 2nd St., 28th Floor
Miami, FL 33131
Tel.: (305) 539-8400
jlee@bsflfp.com
rbaeza@bsflfp.com

Alison L. Anderson, CA Bar No. 275334
725 S Figueroa St., 31st Floor
Los Angeles, CA 90017
Tel.: (213) 995-5720
alanderson@bsflfp.com

SUSMAN GODFREY L.L.P.

Bill Carmody (admitted pro hac vice)
Shawn J. Rabin (admitted pro hac vice)
Steven M. Shepard (admitted pro hac vice)
Alexander Frawley (admitted pro hac vice)
1301 Avenue of the Americas, 32nd Floor
New York, NY 10019
Tel.: (212) 336-8330
bcarmody@susmangodfrey.com
srabin@susmangodfrey.com
sshepard@susmangodfrey.com
afrawley@susmangodfrey.com

Amanda K. Bonn, CA Bar No. 270891
1900 Avenue of the Stars, Suite 1400
Los Angeles, CA 90067
Tel.: (310) 789-3100
abonn@susmangodfrey.com

MORGAN & MORGAN

John A. Yanchunis (admitted pro hac vice)
Ryan J. McGee (admitted pro hac vice)
201 N. Franklin Street, 7th Floor
Tampa, FL 33602
Tel.: (813) 223-5505
jyanchunis@forthepeople.com
rmcgee@forthepeople.com

Michael F. Ram, CA Bar No. 104805
711 Van Ness Ave, Suite 500
San Francisco, CA 94102
Tel: (415) 358-6913
mram@forthepeople.com

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA**

CHASOM BROWN, WILLIAM BYATT,
JEREMY DAVIS, CHRISTOPHER
CASTILLO, and MONIQUE TRUJILLO
individually and on behalf of all similarly
situated,

Plaintiffs,

vs.

GOOGLE LLC,

Defendant.

Case No.: 4:20-cv-03664-YGR-SVK

**PLAINTIFFS' TRIAL PLAN IN
SUPPORT OF MOTION FOR CLASS
CERTIFICATION**

Judge: Hon. Yvonne Gonzalez Rogers
Date: September 20, 2022
Time: 2:00 p.m.
Location: Courtroom 1 – 4th Floor

TABLE OF CONTENTS

| | | |
|-------|---|----|
| I. | Introduction | 1 |
| II. | Scope and Length of Trial | 1 |
| III. | Claims | 2 |
| IV. | Applicable Law | 2 |
| V. | Elements of Plaintiffs’ Claims | 3 |
| VI. | Stipulated Facts | 3 |
| VII. | Scope of Classes | 3 |
| VIII. | Sanctions, Preservation, and Preclusion Rulings | 4 |
| | A. Sanctions | 4 |
| | B. Preservation | 5 |
| | C. Preclusion | 5 |
| IX. | Procedures to Simply Trial Presentation | 5 |
| X. | Common Issues and Evidence | 6 |
| | A. Google’s Form Contract | 6 |
| | B. Google Documentary Evidence | 8 |
| | C. Google Employee Testimony | 9 |
| | D. Plaintiffs’ Testimony | 12 |
| | E. Expert Liability Testimony | 12 |
| | F. Damages Evidence | 14 |
| | G. Injunctive Relief | 18 |
| XI. | Notice Program and Post-Judgment Administration | 19 |
| XII. | Conclusion | 22 |

I. INTRODUCTION

Plaintiffs respectfully submit this Trial Plan in support of their class certification motion.¹ This Trial Plan provides a roadmap to aid the Court in assessing how a trial can be conducted in an efficient and manageable manner. It includes information regarding how Plaintiffs intend, subject to the Court's guidance, to present their claims and seek relief at trial in a way that is consistent with the requirements of Rule 23. While this Trial Plan is meant to serve as a useful roadmap of the key documents and witnesses to be presented at trial, it is not intended to be an all-inclusive, exhaustive list of documents and witnesses as Plaintiffs will continue to evaluate the case as it proceeds to trial.

Plaintiffs seek certification of two classes for purposes of asserting seven claims. Those claims concern Google's collection of private browsing information from ██████████ of Americans who used Chrome Incognito mode (Class 1) and the private browsing modes in Safari, Edge, and Internet Explorer (Class 2) during the period dating back to June 1, 2016 and to the present (the Class Period). Plaintiffs will show at trial, using common proof for the Class Period and for all Class Members, how Google collected and stored private browsing information and used that private browsing information to generate ██████████ in revenues. Google did this in violation of its contracts with Class Members and other laws. Plaintiffs now seek monetary, injunctive, and other relief on behalf of Class Members.

II. SCOPE AND LENGTH OF TRIAL

Plaintiffs propose that all issues be tried together in a single trial. Subject to the Court's guidance and rulings, Plaintiffs will present a combination of live and videotaped testimony from the five named Plaintiffs, Plaintiffs' six experts, and current and former Google employees and other witnesses. The length of the trial will depend in part on the extent to which the parties can streamline the presentation through various stipulations and also any case that Google wishes to present. Excluding jury selection, Plaintiffs' current estimate is that trial can be completed in

¹ Google criticized the *Calhoun* plaintiffs for not submitting a trial plan. See *Calhoun*, 20-cv-5146, Dkt. 429 at 24-25.

approximately 20 court days, with Plaintiffs and Google splitting their time equally.² Subject to the Court’s availability, Plaintiffs are prepared to proceed to trial as early as January 2023.

III. CLAIMS

Plaintiffs seek class certification with seven claims, all of which have survived Google’s motions to dismiss. *See* Dkt. 113 (order denying Google’s first motion to dismiss); Dkt. 363 (order denying Google’s second motion to dismiss); *see also* Dkt. 504 (order granting Plaintiffs’ motion for leave to file their Third Amended Complaint); Dkt. 395-2 (Plaintiffs’ Third Amended Complaint, including Plaintiffs’ seven claims). Plaintiffs’ claims are: (I) violations of the federal Wiretap Act, (II) violations of the California Invasion of Privacy Act (“CIPA”), (III) violations of California’s Comprehensive Computer Data Access and Fraud Act (“CDAFA”), (IV) invasion of Class Members’ privacy and (V) intrusion upon their seclusion in violation of California law, (VI) breach of contract, and (VII) violations of the “unlawful” and “unfair” prongs of California’s Unfair Competition Law (“UCL”).

IV. APPLICABLE LAW

Plaintiffs assert one claim under federal law (Count I) and six claims under state law (Counts II-VII). *See* Dkt. 395-2. Google’s contract with all Class Members throughout the Class Period included a California choice-of-law provision. Dkt. 83-16 at 8; Ex. 15. Google’s California choice-of-law provision reaches “any disputes arising out of or relating to these terms or the Services” (April 14, 2014 – October 24, 2017 Terms of Service and October 25, 2017 – March 30, 2020 Terms of Service) and “all disputes arising out of or relating to these terms, service-specific additional terms, or any related services” (March 31, 2020 – January 4, 2022 Terms of Service). *Id.* Plaintiffs’ state law claims fall within the scope of the California choice-of-law provision because they “aris[e] out of or relat[e] to” Google’s Terms of Service and Google’s services. *See, e.g.,* Dkt. 395-2 ¶¶ 84–88, 224–25, 233–34, 246, 259–60, 268–72, 282. *See also* Motion § II.B.1; Hochman Report § VIII.G (describing how Google implemented relevant processes from California with California-based employees able to access private browsing data in California).

² This assumes cross examinations and the Defendant’s case are of reasonable length.

V. ELEMENTS OF PLAINTIFFS' CLAIMS

Plaintiffs intend to present common evidence establishing the elements of their claims. For the Court's convenience and reference, in Appendix A, Plaintiffs provide a chart summarizing the elements of their seven claims.

VI. STIPULATED FACTS

For many elements of Plaintiffs' claims, Plaintiffs believe that the parties can streamline trial by stipulating to certain facts. Those stipulated facts could include, for example: (1) the Google disclosures related to private browsing during the relevant time period; (2) Google's collection, storage, and use of Class Members' private browsing information; (3) the revenue Google has generated from its collection, storage, and use of Class Members' private browsing information, for purposes of calculating monetary relief; and (4) Google's continuing collection, storage, and use of Class Members' private browsing information, for purposes of any injunctive relief. Expert discovery is concluding, and that discovery may help identify additional factual issues that are undisputed.

VII. SCOPE OF CLASSES

Plaintiffs seek to certify claims on behalf of Class Members nationwide as to Counts I, III, IV, V, VI, and VII of their Third Amended Complaint (Dkt. 395-2): (I) violations of the federal Wiretap Act, (III) violations of California's Comprehensive Computer Data Access and Fraud Act ("CDAFA"), (IV) invasion of Class Members' privacy and (V) intrusion upon their seclusion in violation of California law, (VI) breach of contract, and (VII) violations of the "unlawful" and "unfair" prongs of California's Unfair Competition Law ("UCL"). Consistent with this Court's recent guidance, *see In re Google RTB Consumer Privacy Litigation*, Case No. 4-21-cv-02155-YGR, Dkt. 233 at 17 (N.D. Cal. June 13, 2022), Plaintiffs seek to certify California-resident only classes as to Count II of their Complaint (violations of the California Invasion of Privacy Act ("CIPA")).

Plaintiffs' damages expert has estimated that from the start of the Class Period through the end of 2021, nationwide, there were about [REDACTED] members of the Incognito class (Class 1) and about [REDACTED] members of the class for the Safari, Edge, and Internet Explorer private

browsing modes (Class 2). *See* Lasinski Report ¶ 195, Figure 75. Plaintiffs’ class administration expert (who has been involved with hundreds of class actions) has also detailed how Class Members can be notified. *See* Weisbrot Report § IV. Notification is straightforward in this case because all Class Members are Google account holders, where Google should have contact information. *Id.* ¶ 26.

VIII. SANCTIONS, PRESERVATION, AND PRECLUSION RULINGS

One common issue for trial will be application of the Court’s sanctions, preservation, and preclusion rulings. *See* Dkts. 588, 587, 288-1.

A. Sanctions

After intensive briefing and a full-day hearing, the Court granted in part Plaintiffs’ Motion for Sanctions for Google’s Discovery Misconduct. Dkt. 588. The Court found that Google “with[held] relevant discovery focused on Google’s Incognito-detection bits,” Dkt. 588-1 at 32, which Google developed and used to identify Incognito traffic. This evidence was “relevant to both Plaintiffs’ claims and Google’s defenses” and Google’s withholding of this evidence “prejudiced Plaintiffs’ ability to fully address the assertions by Google, its counsel, and its witnesses” concerning Google’s ability to identify Incognito traffic. Dkt. 588-1 at 29, 32.

As a result, the Court ordered evidentiary sanctions and a jury instruction that would streamline trial: (1) evidentiary sanctions precluding Google from (a) “object[ing] to or present[ing] argument against the timing of the development and implementation of the three Incognito-detection bits at issue or the fact that such bits were implemented,” (b) “offer[ing] or rely[ing] on testimony from Chris Liao, Bert Leung, Mandy Liu, or Quentin Fiard for any purpose,” and (c) “offering or relying on its Supplemental Response to Interrogatory No. 35”; and (2) if “Google’s discovery misconduct is relevant to an issue before the jury,” a jury instruction that (a) “Google failed to disclose to Plaintiffs the names of key Google employees responsible for developing and implementing Google’s Incognito-detection bits” and (b) that “Google failed to disclose relevant data sources reflecting the use of the Incognito-detection bits.” *Id.* This ruling, which Google did not appeal, will inform the presentation of evidence and argument at a class-wide trial.

1 **B. Preservation**

2 On May 20, 2022, based on Plaintiffs’ objections in connection with Google’s preservation
 3 obligations, the Court ordered that “Google may not use the fact that only sampled data, not
 4 complete data, is available to challenge class certification generally or attestations by individuals
 5 that they are members of the class.” Dkt. 587 at 7. The Court also ordered that Google must
 6 preserve certain data. *Id.* That ruling is relevant for purposes of class certification and any class
 7 member attestations presented during any claims process.

8 **C. Preclusion**

9 On October 19, 2020, Plaintiffs served requests for production of “[d]ocuments sufficient
 10 to identify all websites and publishers that use Google Analytics” (RFP No. 50) and “[d]ocuments
 11 sufficient to identify all websites and publishers that use Google Ad Manager (RFP No. 65). Dkt.
 12 288-1. Google refused to produce such documents, and the parties briefed the issue for the Court.
 13 Google argued that its response to Plaintiffs’ Interrogatory No. 5, in which Google identified the
 14 top 25 visited websites for each of Google Analytics and Google Ad Manager, was “sufficient
 15 with respect to providing any potentially relevant information that is responsive to this request.”
 16 Dkt. 281 at 31. The Court ordered that, “before Google can argue or assert that any specific website
 17 did not use” either Google Analytics or Google Ad Manager, “Google must respond to this
 18 interrogatory as to that website at least 30 days in advance of making any such assertion or
 19 argument.” Dkt. 288-1 at 1-2. Fact discovery has ended, and Google never supplemented this
 20 interrogatory response to assert that any specific website did not use Google Analysis or Google
 21 Ad Manager. Google is now precluded from disputing whether any website used Google Ad
 22 Manager or Google Analytics. That is relevant for purposes of class certification, trial, and any
 23 post-trial attestations.

24 **IX. PROCEDURES TO SIMPLIFY TRIAL PRESENTATION**

25 Consistent with the Court’s Standing Order Re: Pretrial Instructions in Civil Cases,
 26 Plaintiffs will seek to reach agreement with Google on issues affecting the conduct of trial. This
 27 will likely include matters such as a proposed order outlining a variety of stipulations regarding
 28 the conduct of the trial, a list of discovery excerpts, audios, and videos likely to be used at trial,

the authenticity and admissibility of documents produced by the parties, a joint set of proposed jury instructions, a joint proposed verdict form, and a joint statement of the case to be read to the jury. The parties previously were able to reach certain agreements regarding the authenticity of documents, including that many will be presumed business records under Federal Rule of Evidence 803(6) (Dkt. 472), and Plaintiffs anticipate further progress on other issues to streamline the trial of the case.

X. COMMON ISSUES AND EVIDENCE

Three core questions underpin all of Plaintiffs' claims:

1. Did Google promise Class Members that using a "private browsing mode" (including Chrome Incognito mode) would prevent Google from collecting, saving, and using their information when browsing non-Google websites?
2. Did Google nevertheless collect, save, and use Class Members' private browsing activity unlawfully?
3. How much did Google profit from its conduct while harming Class Members?

Each of these questions can be answered from common proof. Below, Plaintiffs preview the common proof that answer these core questions and how that evidence will be admitted at trial. For consideration, in Appendix B, Plaintiffs also include an exemplar exhibit list consistent with the Court's format.³

A. Google's Form Contract

The starting point for all of Plaintiffs' claims (and also Google's defenses) is the contract between Google and Class Members, which is subject to common proof and interpretation. This Court already ruled that a form contract between Google and Google account holders exists and is made up of and incorporates: (1) Google's Privacy Policy; (2) Google's "Search & Browse Privately" page; (3) Google's "Chrome Privacy Notice"; and (4) the "Incognito Splash Screen." Dkt. 363 at 13-14, 17; *see also* Schneier Report ¶¶ 278-283 (summarizing the representations made within these documents throughout the Class Period).

³ While certainly not all inclusive, this sample list gives the Court a sense of the key exhibits that will be used at trial.

1 Plaintiffs will introduce Google’s form contract to show that throughout the Class Period
 2 and for all Class Members (all of whom are Google account holders, subject to Google’s form
 3 contract), Google promised that users could “control” what information Google can collect, that
 4 users could exercise that control by using private browsing modes such as Incognito mode, and
 5 that Google would not collect users’ private browsing information.

6 As summarized by the Court, Google’s form contract includes the following statements
 7 representing that private browsing mode prevents Google from collecting users’ data:

- 8 • “The Incognito Splash Screen’s list of entities that can view a user’s activity in
 9 private browsing mode, which omits Google and instead lists: ‘Websites you visit;
 Your employer or school; Your internet service provider.’”
- 10 • “The Incognito Splash Screen’s statement that: ‘Now you can browse privately,
 11 and other people who use this device won’t see your activity.’”
- 12 • “The Incognito Splash Screen’s Statement that: ‘Chrome won’t save . . . [y]our
 13 browsing history [or] cookies and site data.’”
- 14 • “The ‘Search & Browse privately’ page’s statement that: ‘You’re in control of what
 15 information you share with Google when you search. To browse the web privately,
 16 you can use private browsing.’”
- 17 • “The Chrome Privacy Notice’s statement that: ‘You can limit the information
 18 Chrome stores on your system by using Incognito mode or guest mode. In these
 19 modes, Chrome won’t store certain information, such as: ...Basic browsing history
 information like URLs, cached paged text, or IP addresses of pages linked from the
 websites you visit [and] Snapshots of pages that you visit.’”
- 20 • “Google’s Privacy Policy’s statement that: ‘You can...choose to browse the web
 21 privately using Chrome in Incognito mode. And across our services, you can adjust
 22 your privacy settings to control what we collect and how your information is used.’”

23 Dkt. 363 at 20-21. The Court further held that: “Given the Court’s previous conclusion regarding
 24 each of these individual statements, a reasonable user, reading Google’s contract with Plaintiffs as
 25 a whole, could easily conclude that Google promised that using ‘private browsing mode’ would
 26 prevent Google from collecting Plaintiffs’ data.” Dkt. 363 at 21. This form contract will define the
 27 scope of any consent provided by Class Members regardless of what any users knew or believed
 28 about Google’s conduct. That is particularly true here where Google’s form contract throughout
 the entire Class Period expressly waived any implied consent defense, providing: “We will not
 reduce your rights under this Privacy Policy without your explicit consent.” Dkt. 83-1 at 12.
 Plaintiffs intend to present these same Google statements and promises to the jury to support

1 Plaintiffs' claims.

2 **B. Google Documentary Evidence**

3 At trial, Plaintiffs will seek to offer into evidence internal Google documents as common,
 4 classwide proof that, internally, Google employees acknowledged that Google's disclosures,
 5 branding, and marketing led reasonable users to believe, erroneously, that private browsing modes
 6 prevent Google from collecting, saving, and using their data. Plaintiffs will also offer Google's
 7 documents demonstrating that Google throughout the Class Period collected private browsing data
 8 despite what Google employees described as "common" misconceptions.

9 For example, there are documents in which Google employees admitted that Google was
 10 making and breaking promises regarding private browsing. *See, e.g.*, Ex. 30 at -21 (expressing
 11 concern that Google might be "making privacy worse by collecting Incognito when the user has
 12 clearly told Chrome that it wants to be private" and thereby not "actually deliver[ing] on the
 13 promise of being private"); Ex. 12 at -02 (with Incognito, "[w]e are over-promising and under-
 14 delivering"); Ex. 37 at -80 (discussing Incognito as a "promise we don't keep"); Ex. 39 at -
 15 64 ("we also might change the [Incognito] name and functionality to overcome the
 16 'overpromising' issue"); Ex. 40 ("[r]eneging on the promise that incognito mode doesn't leave
 17 traces of your browsing session seems bad"); Ex. 41 at -77 (discussing "gap between our promises
 18 about Chrome Incognito mode, their delivery, and user expectations"); Ex. 38 at -17 (noting need
 19 to "re-think incognito branding and promises").

20 For consideration, Appendix B includes a sample exhibit list with 35 documents produced
 21 by Google that Plaintiffs intend to present at trial, including short summaries of those documents.⁴
 22 Appendix B includes, for example, admissions by Google employees and executives that Incognito
 23 was "not truly private" (Entry 31, Ex. 1 at -67), how Incognito was "radioactive" and "effectively
 24 a lie" (Entry 4, Ex. 2 at -26), and how, aware of the problems and misconceptions fatally plaguing
 25 Incognito mode, Google CEO Sundar Pichai decided that he "didn't want to put incognito under
 26 the spotlight" (Entry 22, Ex. 10 at -93). Google has stipulated to the authenticity of all of these

27 ⁴ This is not intended to be an all-inclusive exhibit list at this early stage but instead meant to
 28 provide the Court with a sample.

documents. *See* Dkt. 472. Copies of the documents cited in Appendix B are attached to the concurrently filed Mao Declaration.

C. Google Employee Testimony

Plaintiffs intend to either seek live testimony or present videotaped deposition testimony excerpts from current and former Google employees. This common proof will demonstrate that Google’s Incognito disclosures, branding, and marketing were known to be misleading by Google, and Google nevertheless utilized tracking beacons that caused users’ browsers to send Google information about users’ browsing on third-party websites even when the users were in private browsing mode. Plaintiffs intend to cover for example:

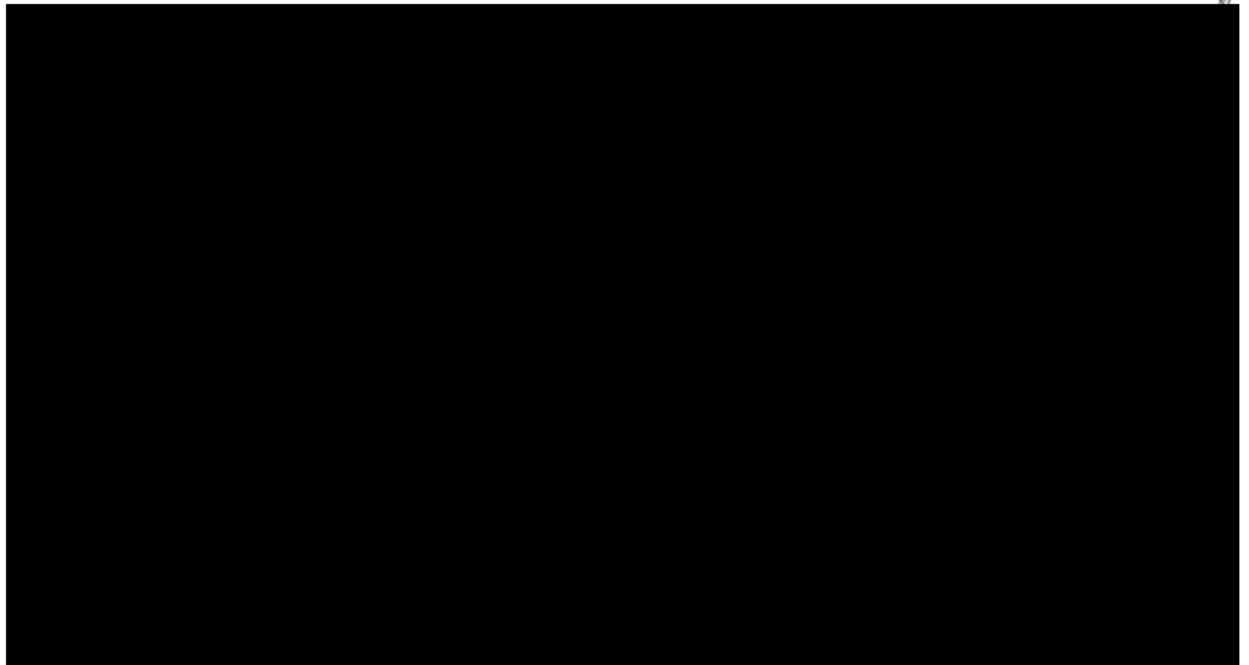
Chris Palmer: Google employee Chris Palmer sent emails and testified about the Incognito “war” waged internally at Google, with Mr. Palmer and others recognizing that Incognito “has always been a misleading name” and is “effectively a lie.” Ex. 4 at -65, Ex. 2, Ex. 17. Both before and throughout the Class Period, Mr. Palmer knew that “people don’t and indeed cannot understand Incognito’s guarantee(s)” and people have been instead “operating under a false sense of privacy.” Ex. 42 at -66, Ex. 43 at -55. Mr. Palmer and others tried to fix this, with proposals going all the way to Google CEO Sundar Pichai, but Google never implemented those proposed changes. Ex. 7 at -04, Ex. 10 at -93; *see also* Ex. 44 at -09 (Mr. Palmer wrote “the blame for people’s misconceptions about Incognito mode is due to that name and branding, as I have argued repeatedly”); Ex. 17 at 146:15-21 (testifying that Incognito mode is not only confusing for people who use Incognito mode but also “people who use other browsers”).

Ramin Halavati: Google employee Ramin Halavati testified about Google’s tracking of Incognito browsing, with a Google logging system containing the “ground truth” in terms of Incognito usage. Ex. 45 at 172:8-18; *see also* Ex. 32 at -22. Mr. Halavati also authored numerous papers describing for example how “the spy icon may be misleading” (Ex. 46 at -97), there “is a gap between our Chrome Incognito mode, their delivery, and user expectations” (Ex. 41 at -77), and describing “common misconceptions” about private browsing modes, including the misconception that it “hides browsing activity from Google” (Ex. 9 at -82). He also acknowledged internally, to other Google employees, that Google is “logging all user activities in incognito mode

1 server-side, and that is more or less linkable to users['] signed-in data.” Ex. 47 at -75; *see also* Ex.
2 48 at -01 (“IP can be used to join the authenticated and incognito sessions”).

3 **AbdelKarim Mardini:** Google employee Abdelkarim Mardini was and still is a top
4 executive in Google’s Chrome group. He was part of the Google team that evaluated the financial
5 impact to Google of blocking third-party cookies by default in Incognito mode, calculated at [REDACTED]
6 [REDACTED] in 2021 alone. Ex. 31 at -07. In 2021, Mr. Mardini was also part of efforts to change
7 Google’s disclosures due to “misconceptions about Incognito” (Ex. 49 at -51) but that never
8 happened. Mr. Mardini was also part of discussions regarding changes to Incognito mode “to also
9 offer some privacy towards Google” (Ex. 50 at -86) and “delete logs from Incognito browsing”
10 (Ex. 51 at -92), and Mr. Mardini was the one who wrote about Google CEO Sundar Pichai’s desire
11 to not “put incognito under the spotlight” (Ex. 10 at -93).

12 **Rory McClelland:** Former employee Rory McClelland testified about Google’s failure to
13 remedy known problems with Incognito mode. Mr. McClelland acknowledged internally that the
14 Incognito screen was (and still is) problematic in part because it omits Google from the list of
15 entities that can view private browsing information, and so he recommended redesigning the
16 Incognito screen to clarify that “You are protected from other people who use this device” but
17 “You are NOT protected from Google.” Ex. 52:



Google executives rejected Mr. McClelland's proposal. Ex. 53 (McClelland Tr.) 58:19-59:6. Mr. McClelland also testified that Google could have implemented a "Do Not Track protocol" for Incognito mode, but Google executives chose not to because that would decrease Google's revenues. *Id.* 126:14-132:13. Mr. McClelland also testified that "it's possible for Google to join regular and Incognito sessions" based on how Google stores information. *Id.* 212:13-212:24.

Sundar Pichai: Plaintiffs seek testimony from Google CEO Sundar Pichai, with further briefing next month on whether they may depose Mr. Pichai. Dkt. 602. Mr. Pichai led the Google team that launched Incognito in 2008, which knew then that "[p]eople didn't understand Incognito." Ex. 54 at -87. A 2015 Google document reported that people were "confused" and "unsure about [Incognito's] true functionality" (Ex. 55 at -14) and that "contributed toward the Privacy/Policy presentation to Sundar [Pichai]." Ex. 55 at - 11. Then, in 2016, it was Mr. Pichai who proposed to use the same Incognito name and icon with other products, which Google employees recognized would "exacerbate the confusion, which is already bad." Ex. 7 at -04. In 2019, Mr. Pichai was apprised of "known misconceptions about protections Incognito mode provides" and warned not to "use the words private, confidential, anonymous, off-the-record when describing benefits of Incognito mode." Ex. 20 at -68.C. But rather than attempt to fix Google's Incognito problem, Mr. Pichai decided not to "put incognito under the spotlight." Ex. 10 at -93. And although Mr. Pichai initially expressed "enthusiasm" for an [REDACTED] (Ex. 56 at -23) with "anti-tracking" elements (Ex. 57 at -79), Google never launched [REDACTED], instead continuing to collect users' private browsing information. Mr. Pichai will provide unique testimony concerning the reasoning for key decisions regarding the conduct at issue. *E.g.*, Ex. 58 at -49 (referring to decision to expand Incognito branding as a "Sundar level decision"); Ex. 59 at -37 (stating Mr. Pichai "brought up the idea"); Ex. 60 at -88 (stating "Sundar led the discussion" on "whether we should block 3P cookies"); Ex. 61 at -09 (discussing "meeting with Sundar" where team received Mr. Pichai's "[o]verall approval of plan on data disclosures, . . . [REDACTED] controls - 3P / Incognito controls"). Testimony may be the only evidence for some of these key decisions, with Mr. Pichai instructing Google employees not to communicate in writing. *See, e.g.*, Ex. 11 at -77 (Mr. Pichai instructing "pls don't discuss more in this thread"); Ex. 62 at -03 (Google

employee instructing for Mr. Pichai meeting “don’t need to share any further....trying to stay off notes”).

D. Plaintiffs’ Testimony

At trial, Plaintiffs intend to present testimony from their five named Plaintiffs. The named Plaintiffs will testify that reasonable Google users such as themselves interpreted Google’s disclosures to mean that Google would not collect, save, and use Class Members’ private browsing data. The named Plaintiffs, like all other Class Members, enabled private browsing mode, including Incognito Mode, when they browsed the internet to, in part, prevent Google from collecting, saving or using their private browsing data. Plaintiffs and the Class Members were harmed by Google’s surreptitious collection and use of their private browsing data without their consent. Plaintiffs have submitted declarations in support of their class certification motion.

E. Expert Liability Testimony

At trial, Plaintiffs intend to present testimony from their four liability experts. Plaintiffs provided detailed reports for each of these experts, including executive summaries at the start of each report. Professor Schneier, Mr. Hochman, and Mr. Keegan each submitted opening reports, and all four experts (including Mr. Nelson) submitted rebuttal reports addressing portions of Google’s opening expert reports. With their expert testimony, based on common proof, Plaintiffs will establish their entitlement to relief. Consistent with their expert reports, Plaintiffs anticipate the following testimony at trial:

Jonathan Hochman: Mr. Hochman is the founder of Hochman Consultants, an agency that provides clients with online security, ecommerce, and advertising services. Among other topics, Mr. Hochman will testify about the technical processes by which Google, on a classwide basis, collects, stores, and uses private browsing information, including for purposes of monetizing that private browsing information. Hochman Report §§ A, D, E. Mr. Hochman will also describe the nature and contents of the private browsing information uniformly collected by Google and explain how the data is tied to unique identifiers and other information about users. *Id.* § F. In addition, having analyzed the data that Google produced to Plaintiffs through the Special Master process, Mr. Hochman will explain how Google systematically collects and tracks Incognito

browsing activity, where Google's Incognito "detection bits" (the subject of the Court's prior sanctions order) reliably detected Incognito traffic with [REDACTED] accuracy. Hochman Rebuttal ¶ 28. Using the same data from the Special Master process, Mr. Hochman will explain how, for all Class Members, private browsing data within Google's logs can be easily joined with users' Google accounts. *Id.* §§ V.A, D. Mr. Hochman will also explain how Google designed Chrome and search so that people clicking on search results would have their searches and search terms included and tracked in the browser request to the non-Google websites, including when people use private browsing. When people visit non-Google websites in private mode, the search terms are copied by Google scripts for Google servers from the browsers. Hochman Rebuttal ¶¶ 39-42; *see also* Ex. 63 at 203-04; TAC ¶ 208, Dkt. 395-2.

Professor Bruce Schneier: Professor Schneier, a lecturer and fellow at the Harvard Kennedy School, is a security technologist who researches, writes, and speaks about computer security and Internet security, as well as the economic, psychological, and sociological aspects of security and privacy. Professor Schneier studies user behavior and human factors related to security and privacy. Professor Schneier studies user behavior and human factors related to security and privacy, and his 2014 book *Data and Goliath* explores people's relationship with privacy and their behaviors regarding privacy. Professor Schneier will provide important context for the jury regarding the disclosures at issue in this case, the existence of reasonable expectations of privacy in connection with private browsing communications, and why Google's collection, storage, and use of that information is highly offensive. For example, Professor Schneier will describe how the rise of the Internet and surveillance business models have created significant threats to online privacy, making it more important for users to have a refuge from pervasive tracking. Schneier Report §§ IV.2-3. Professor Schneier will also offer opinions about Google's disclosures, including how they fail to disclose Google's collection of private browsing information and instead falsely present private browsing modes as something that would provide actual privacy, including from Google. *Id.* §§ 11-12.

Mark Keegan: Mark Keegan is a survey expert who has personally conducted over 1,000 consumer surveys reaching more than 250,000 consumers. For this case, Mr. Keegan conducted two surveys of people who used one or more of the private browsing modes at issue (Chrome,

Safari, Edge, and Internet Explorer) during the Class Period. Mr. Keegan's first survey provides common statistical evidence, including (1) for each browser at issue, the proportion of users who use that browser's private browsing mode; and (2) the proportion of such users who also have a Google account (a prerequisite for class membership). Keegan Report Opinion 3. Mr. Keegan's second survey provides common evidence demonstrating that, based on their experience and review of certain disclosures (including the Incognito Splash Screen for Incognito users), of users did not understand or believe that they consented to Google's collection and storage of their private browsing data. See Keegan Rebuttal Report, Opinions 6-7, ¶¶ 7-8, 156-92. This survey constitutes common, classwide evidence that users reasonably understood the contract to promise that Google would not collect their private browsing data. Mr. Keegan will also explain why Google's competing survey is methodologically flawed, including because Google's expert failed to screen out participants who admitted to knowing about this lawsuit (and therefore knew about Google's collection of private browsing data). Keegan Rebuttal, Opinion 7.

David Nelson: Mr. Nelson is a former FBI agent with twenty-four years of experience in cybercrime investigations. Mr. Nelson will rebut Google's technical expert (Professor Georgios Zervas), where Professor Zervas seeks to offer testimony suggesting that private browsing information is not saved or capable of being linked to a user or her device. Mr. Nelson will explain why such testimony is misleading, particularly because Professor Zervas does not even address how private browsing information saved and stored by Google is in fact tied to user identifiers such as IP address that can be used to join private browsing information to specific users. Nelson Report ¶ 16. In particular, Mr. Nelson will describe how Google routinely produces browsing data tied to IP address information in response to government subpoenas, and that Mr. Nelson and his team were able to use such browsing data to identify people, including in some cases private browsing data tied to IP address. *Id.* ¶¶ 31-37.

F. Damages Evidence

At trial, Plaintiffs will also present expert testimony and other evidence regarding the calculation of the monetary relief and statutory damages they seek. The evidence presented will also bear on the appropriateness of awarding punitive damages and nominal damages.

1 Plaintiffs' damages expert Michael Lasinski is a Certified Public Accountant with twenty-
2 seven years of experience evaluating the financial aspects of intellectual property for government
3 entities, corporations, and law firms. Mr. Lasinski calculated specific and aggregated amounts for
4 unjust enrichment (in the form of non-restitutionary disgorgement of profits) and actual damages
5 (in the form of restitution), and Mr. Lasinski's report includes an executive summary detailing
6 those calculations, which are summarized below.

7 Unjust Enrichment: Plaintiffs allege that once Google misappropriated Plaintiffs' private
8 browsing data and took away their ability to browse privately, Google then generated [REDACTED]
9 [REDACTED] in profit with what it misappropriated. Plaintiffs accordingly seek non-restitutionary
10 disgorgement damages, which are available for at least their contract, CDAFA, and federal
11 Wiretap Act claims. *See* Motion § II.B.4.a (citing authorities).

12 Plaintiffs' calculation of non-restitutionary disgorgement damages begins with Google's
13 own undisputed analysis of the financial impact to Google of blocking one of its methods for
14 tracking users in Incognito mode—something called “third-party cookies.” Lasinski Report § 7.1
15 Plaintiffs intend to present documents and testimony regarding how Google employees concluded
16 that blocking third-party cookies by default in Chrome Incognito mode would result in Google
17 losing about [REDACTED] in 2021. *E.g.*, Ex. 64 at -35. Relying on that internal Google financial
18 model as a starting point, and after making certain downward adjustments to exclude profits
19 outside the scope of this case, Mr. Lasinski used Google's public financial documents and other
20 discovery to calculate Google's unjust enrichment by way of the Google tracking and advertising
21 code that enables Google to collect private browsing information from members of each of the two
22 Classes. Lasinski Report § 7.

23 The model and calculations are detailed in Mr. Lasinski's report, where Mr. Lasinski
24 concludes that Google was unjustly enriched by [REDACTED] from the start of the Class Period
25 through the end of 2021, including [REDACTED] for Class 1 (the Incognito class). If permitted, and
26 assuming a trial in 2023, Mr. Lasinski could update this calculation for the period through the end
27 of 2022. As described below, Plaintiffs intend to distribute any aggregate unjust enrichment award
28 to class members on a pro rata or per capita basis.

1 Actual Damages: To prove actual damages, Plaintiffs will proffer evidence regarding how
 2 Google itself values the opportunity cost of users giving up privacy from Google, in addition to
 3 the value of the private browsing data Google acquired and misappropriated. Plaintiffs will present
 4 documents and testimony regarding Google’s own calculations for this restitutionary value,
 5 including the value that Google assigned when purchasing access to users’ online activity and data
 6 with its Ipsos Screenwise Panel. Through this Google program, which was the subject of document
 7 production and deposition testimony, Google determined how much to pay participants each
 8 month for full access to browsing information—private or otherwise—on their devices. Lasinski
 9 Report ¶¶ 143-50 (describing program and payments). Mr. Lasinski will present an actual damages
 10 calculation using the lower-bound of Google’s scale (a \$3 monthly payment) as a conservative
 11 valuation of how much Google would have needed to pay to purchase monthly access to the private
 12 browsing activity it intercepted throughout the Class Period. *Id.* ¶ 165. Mr. Lasinski also used
 13 common evidence in the form of data obtained from Google to quantify the number of unique
 14 monthly private browsing instances during the Class Period and through the end of 2021, i.e., a
 15 monthly measurement that Google uses to track devices that use private browsing. *Id.* ¶ 166. That
 16 data is from a Google data system that Google employees describe as the “ground truth.” Ex. 32
 17 at -22. Mr. Lasinski made certain downward adjustments to calculate the relevant number of
 18 monthly instances for each of the two Classes and then multiplied that amount by \$3 per month.
 19 With that analysis, starting with Google’s own data, Mr. Lasinski calculated approximately [REDACTED]
 20 [REDACTED] as the aggregate lost value of Class Members’ private browsing data from the start of the
 21 Class Period through the end of 2021, including [REDACTED] for Class 1 and [REDACTED] for
 22 Class 2. *Id.* ¶ 184. If permitted, and assuming a trial in 2023, Mr. Lasinski could update this
 23 calculation for the period through the end of 2022.

24 Statutory Damages: Plaintiffs seek statutory damages under the federal Wiretap Act (Count
 25 One) and CIPA (Count Two), both of which allow for recovery of statutory damages as an
 26 alternative to actual damages. Under the federal Wiretap Act, the Court may assess as damages
 27 whichever is the greater of: (a) the sum of the actual damages suffered by the plaintiff and any
 28 profits made by the violator as a result of the violation; or (b) statutory damages—the greater of

(i) \$10,000 or (ii) \$100 a day for each day of violation. 18 U.S.C. § 2520(c)(2). Under CIPA, damages are the greater of \$5,000 or three times the amount of actual damages, if any, sustained by the plaintiff, though proof of actual damages is not necessary for liability. Cal. Penal Code § 637.2(a). As this Court recognized in its March 2021 order denying Google’s motion to dismiss, “each interception is a separate violation” for both the Wiretap Act and CIPA. Dkt. 113 at 24.

The Wiretap Act and CIPA also prohibit attempted interceptions. *See* Cal. Penal Code § 631(a) (prohibiting “attempts to read, or to learn the contents or meaning of any message, report, or communication” as well as “attempts to use” any information obtained in violation of the statute); 18 U.S. Code § 2511(1)(a) (applying to any person who “endeavors to intercept” communications in violation of the statute). In addition to statutory damages for Google’s actual interceptions, Plaintiffs therefore seek statutory damages for a single violation against each member of Class 1 based on Google developing and distributing Chrome Incognito to each of them, and designing Chrome Incognito such that it would not prevent Google’s tracking beacons from collecting Class Members’ private browsing information.

While Mr. Lasinski does not offer any opinion regarding what damages rate the Court should use (e.g., whether \$100 or \$10,000), he proffers four possible bases to which the Court may apply its chosen rate to Google’s violations. All four bases rely on data produced by Google, which Google employees refer to internally as the “ground truth” data for quantifying Incognito traffic, Ex. 32 at -22, which Mr. Lasinski then used to calculate the following through the end of 2021:

1. The total number of individual pageloads in Chrome Incognito mode and the other private browsing modes at issue (Safari, Edge, and Internet Explorer);
2. The total number of unique monthly private browsing instances (“UMPBI”), with one UMPBI referring to a specific browser that used a given private browsing mode at least one time in a month (i.e., if a person regularly used Incognito on her bedroom computer from January – November, but was away for all of December, that would count as 11 UMPBI);

3. A more conservative calculation of unique private browsing instances equivalent to the peak UMPBI for one month (i.e., the month during the class period where total UMPBI was highest); and

4. The total number of Class Members for each of the two Classes (i.e., a single statutory violation per Class Member).

Lasinski Report § 9. All four of these potential bases would enable the Court to calculate statutory damages in the aggregate starting with Google's "ground truth" data.

If the Court were to for example award statutory damages using the fourth calculation, on a per Class Member basis, that would be a basis to award one statutory damages amount (e.g., whether \$100 or \$10,000) for each Class Member. Alternatively, should the Court decide to address statutory damages under Rule 23(c)(4), Class Members could separately by attestation present information to calculate the number of violations to which they were subjected.

Punitive Damages: Plaintiffs do not seek a separate phase for punitive damages, as the entitlement to punitive damages and the amount of any such damages can be determined based on the same evidence described above. Should any punitive damages be awarded, Plaintiffs will also seek to have such damages awarded pro rata or per capita across the class.

G. Injunctive Relief

Plaintiffs will also present evidence to support their request for injunctive relief. Mr. Hochman will describe how Google has continued to collect, store, and use private browsing information even after this lawsuit was filed, which Google does not dispute. Hochman Report §§ VIII.A, D, E. Mr. Hochman will also explain that Google could redesign its tracking beacons and Chrome Incognito to prevent Google's collection of private browsing information and that Google is capable of purging its systems of the private browsing data that it improperly collected. Hochman Report §§ VIII.K-L. Through documentary evidence and testimony, Plaintiffs will seek to establish the importance not only of stopping Google's continued collection of private browsing information but also addressing the massive amount of private browsing data that Google has accumulated over the years and continues to maintain for its own financial benefit. For example, according to Mr. Hochman's analysis, Google in 2017 was storing [REDACTED] of private

browsing information, which equates to [REDACTED].

Hochman Report ¶ 313.

Any injunctive relief should also include ordering Google to stop relying on any of the “dozens of Google [] products” that Google admits to developing with private browsing data. Dkt. 411-1 at 12. Plaintiffs sought discovery on “Google’s use of information collected from users within a private browsing mode for purposes of improving and developing Google services, products, and algorithms.” *Id.* In briefing with the Court, Google objected on the ground that this discovery request “would implicate dozens of Google business units and products.” *Id.* Google has therefore not identified all services, products, and algorithms that have been improved by Google’s use of private browsing information.

More recently, as a result of the Court’s order sanctioning Google for discovery misconduct, Google was forced to finally disclose what Google now claims is the full list of logs that contain Google’s Incognito detection bits. On June 14, 2022, Google informed Plaintiffs that, in addition to the [REDACTED] logs that the Court was already aware of, Google uses these bits within [REDACTED] additional logs, including to perform “analysis and testing” such as “modeling to predict ad revenues.” Ex. 86 ¶¶ 6-7. Plaintiffs also seek injunctive relief regarding any additional uses of data tagged with these Incognito detection bits.

XI. NOTICE PROGRAM AND POST-JUDGMENT ADMINISTRATION

With respect to any aggregate award against Google, Plaintiffs will employ a generally applicable, classwide methodology to divide any recovery among Class Members. Consistent with the process followed in other class cases, Plaintiffs will present a notice program and claims administration protocol for the Court’s review and approval, which would govern the pre-trial notice program as well as post-judgment submission, processing, and resolution of claims with the goal of maximizing Class Member participation and making recovery simple and straightforward.

Plaintiffs have already retained Mr. Weisbrot, an experienced and well-regarded expert who provided the substance for both a pre-trial notice program and post-judgment notification and administrative process. *See* Weisbrot Report. Mr. Weisbrot has been involved with the administration of many other class actions in this District and nationwide, including cases with

Google involving millions of Google account holders. *Id.* ¶¶ 19, 25. In his expert report, Mr. Weisbrot explains that notification in this case is straightforward because the classes are limited to Google account holders, meaning that Google should have Class Member email addresses. *Id.* Opinions 1, 4. It is therefore possible to provide email notification and directions for filling out an online claims form. This approach is especially useful given the large number of Google account holders who use private browsing. *See* Ex. 36 at -22 (“Incognito mode is used by [REDACTED] of Chrome users, and [REDACTED] use it at least once per week.”); Keegan Report Opinion 3 (providing statistics regarding the percentage of Google account holders that use each of the private browsing modes at issue). Because the classes are limited to Google account holders, Google could require claimants to “sign in” to verify their identity and preclude claimants from submitting duplicate claims.⁵ In any event, as explained in Plaintiffs’ Motion and based on established Ninth Circuit precedent, since Google’s liability will be determined in the aggregate, and Google will have no claim to any leftover damages, Google has no due process interest in ensuring that all Class Members come forward, whether any given individual is a rightful Class Member, nor how to distribute damages. Motion §§ II.B.4.e; II.C.

Plaintiffs’ damages expert, Mr. Lasinski, has also explained how any aggregate award can be readily apportioned across and among Class Members. Lasinski Report ¶¶ 196-98. First, any monetary award can be divided by the total number of unique monthly private browsing instances associated with Class Members during the Class Period, which Mr. Lasinski has already quantified using Google’s “ground truth” data. The monetary recovery could then be disbursed pro rata among Class Members based on the number of unique monthly private browsing instances attributable to each Class Member. Class Members can easily and readily provide that information by disclosing the number of months during the Class Period during which they used one or more devices to browse privately and specifying the private browsing modes they used (Chrome, Safari, Edge, and/or Internet Explorer). This approach obtains relevant information for purposes of

⁵ Mr. Weisbrot also proposes numerous supplementary notice procedures, including programmatic display advertising, and social media, video, and radio campaigns. *Id.* § IV.C.

1 apportionment while also being respectful of Class Members' privacy (and not demanding that
2 they disclose which websites they visited privately).

3 Mr. Lasinski also describes how Google's unjust enrichment is attributable to revenue that
4 Google earns by tracking and modeling ad conversions—revenue created by Google using private
5 browsing data in ways that go beyond specific user actions. Lasinski Report § 7.4.1, Schedule 8.1.
6 As explained by Mr. Hochman, Google uses private browsing information to feed Google's
7 machine learning algorithms for tracking and modeling ad conversions, which Google then uses
8 to upcharge its customers. Hochman Report ¶ 202. With these algorithms, fueled by private
9 browsing data, Google benefits from data from users who both do and do not convert because
10 Google uses that data to predict which users may (or even will) convert (which is the enrichment
11 to Google). Hochman Report ¶ 205. Google's conversion tracking revenues are tied to Google's
12 ability to collect and store user browsing data more broadly as opposed to discrete examples of
13 particular users converting. Google benefits from the data collection in the aggregate, and its own
14 employees calculated just days preceding this lawsuit the portion of this Google-generated revenue
15 attributable to private browsing.

16 As explained by Mr. Hochman, if required or permitted by the Court, Google's records (to
17 the extent preserved) could be used to verify claims. Hochman Report ¶¶ 299-307; Hochman
18 Rebuttal Opinion 5. To the extent Google has chosen not to preserve such data that could be used
19 to verify a class member's claim, this Court has ruled that "Google may not use the fact that only
20 sampled data, not complete data, is available to challenge class certification generally or
21 attestations by individuals that they are members of the class." Dkt. 587 at 7. Alternatively, as
22 explained by Mr. Lasinski, damages can be distributed on a per capita basis by dividing any
23 aggregate award by the total number of Class Members, which Mr. Lasinski has calculated as [REDACTED]
24 [REDACTED] members of the Incognito class (Class 1) and about [REDACTED] members of the class for
25 the Safari, Edge, and Internet Explorer private browsing modes (Class 2). Lasinski Report ¶¶ 194-
26 97.

XII. CONCLUSION

As set out in this Trial Plan, Plaintiffs respectfully seek the opportunity to use common, classwide evidence to establish liability and damages, where trying this matter as a class action is consistent with Rule 23's requirements and the due process rights of the parties while assuring a streamlined and efficient trial.

Dated: June 20, 2022

Respectfully submitted,

By: /s/ Mark Mao

Mark C. Mao (CA Bar No. 236165)
mmao@bsflp.com
Beko Reblitz-Richardson (CA Bar No. 238027)
brichardson@bsflp.com
Erika Nyborg-Burch (CA Bar No. 342125)
Enyborg-burch@bsflp.com
BOIES SCHILLER FLEXNER LLP
44 Montgomery Street, 41st Floor
San Francisco, CA 94104
Tel.: (415) 293 6858
Fax: (415) 999 9695

David Boies (admitted *pro hac vice*)
dboies@bsflp.com
BOIES SCHILLER FLEXNER LLP
333 Main Street
Armonk, NY 10504
Tel: (914) 749-8200

James Lee (admitted *pro hac vice*)
jlee@bsflp.com
Rossana Baeza (admitted *pro hac vice*)
rbaeza@bsflp.com
BOIES SCHILLER FLEXNER LLP
100 SE 2nd Street, Suite 2800
Miami, FL 33131
Tel.: (305) 539-8400
Fax: (305) 539-1307

Alison L. Anderson (CA Bar No. 275334)
alanderson@bsflp.com
BOIES SCHILLER FLEXNER LLP
725 S. Figueroa Street, 31st Floor
Los Angeles, CA 90017

1 Tel.: (213) 629-9040

2 Michael F. Ram (CA Bar No. 104805)
3 mram@forthepeople.com
4 MORGAN & MORGAN
5 COMPLEX LITIGATION GROUP
6 711 Van Ness Avenue, Suite 500
7 San Francisco, CA 94102
8 Tel.: (415) 358-6913

9 John A. Yanchunis (admitted *pro hac vice*)
10 jyanchunis@forthepeople.com
11 Ryan J. McGee (admitted *pro hac vice*)
12 rmcgee@forthepeople.com
13 Ra O. Amen (admitted *pro hac vice*)
14 ramen@forthepeople.com
15 MORGAN & MORGAN, P.A.
16 201 N Franklin Street, 7th Floor
17 Tampa, FL 33602
18 Tel.: (813) 223-5505

19 Amanda Bonn (CA Bar No. 270891)
20 abonn@susmangodfrey.com
21 SUSMAN GODFREY L.L.P.
22 1900 Avenue of the Stars, Suite 1400
23 Los Angeles, CA 90067
24 Tel.: (310) 789-3100

25 Bill Carmody (admitted *pro hac vice*)
26 bcarmody@susmangodfrey.com
27 Shawn J. Rabin (admitted *pro hac vice*)
28 srabin@susmangodfrey.com
Steven Shepard (admitted *pro hac vice*)
sshepard@susmangodfrey.com
Alexander P. Frawley (admitted *pro hac vice*)
afrawley@susmangodfrey.com
SUSMAN GODFREY L.L.P.
1301 Avenue of the Americas, 32nd Floor
New York, NY 10019
Tel.: (212) 336-8330

Attorneys for Plaintiffs

Trial Plan Appendix A: Elements of Legal Claims

| Claim | Elements | Predominance |
|---|--|---|
| Count One: Federal Wiretap Act, 18 U.S.C. § 2510 <i>et seq.</i> | Intentionally | <u>Common.</u> Whether Google acted intentionally is common to all class members and will be proven through Google documents, communications, and software applications that apply to the entire class. |
| | Intercepted, attempted to intercept, endeavored to intercept, or procured any other person to intercept or endeavor to intercept | <u>Common.</u> Whether Google did, attempted to, endeavored to, or procured any other person to intercept any communication by collecting private browsing communications between class members and non-Google websites, is common to all class members. How Google intercepted these communications was common to all class members and will be proven through the use of expert testimony by Mr. Hochman. |
| | Any wire, oral, or electronic communication | <u>Common.</u> Whether an individual's browsing information is a communication is common to all class members that does not depend on the individual's particular internet browsing. |

| | | |
|---|---|---|
| Count Two: California Invasion of Privacy Act (CIPA), Cal. Penal Code § 631 | Used any machine, instrument or contrivance; | <u>Common.</u> How Google intercepted communications--through the use of their tracking beacons--is a common question of fact for all class members as Google account holders that used private browsing modes. |
| | To intentionally; | <u>Common.</u> Whether Google acted intentionally is common to all class members, and will be proven through Google's documents and internal communications. |
| | (a) Intercept the content of a communication over any telegraph or telephone wire, line, cable, or instrument; or (b) Read, attempt to read, or learn the contents or meaning of any message, report, or communication; | <u>Common.</u> Whether Google intercepted any communication by collecting private browsing communications between class members and non-Google websites, is common to all class members. How Google intercepted these communications was common to all class members and will be proven through the use of expert testimony by Mr. Hochman. |
| | While the message, report, or communication is in transit or passing over any wire, line or cable; | <u>Common.</u> Whether Google intercepted Plaintiffs' browsing information while the communication was in transit or passing over a wire is common to all class members. |
| | Without the consent of all parties to the communication | <u>Common.</u> Google's arguments regarding consent are common to all class members, likely turning on language in Google's form contracts and broad categories of user actions. |

| | | |
|---|---|---|
| Count Two: California Invasion of Privacy Act (CIPA), Cal. Penal Code § 632 | Google used an electronic amplifying or recording device; | <u>Common.</u> Whether Google used an amplifying or recording device by collecting and storing Plaintiffs' private browsing information is common to all class members. |
| | The communication was confidential, i.e., at least one party to the conversation carried an objectively reasonable expectation that the conversation was not being overheard or recorded. | <u>Common.</u> The question of whether the communication was confidential is based on an objectively reasonable expectation of privacy, and not an individualized subjective standard. Thus, it is common to all class members. |
| Count Three: Comprehensive Computer Data Access and Fraud Act (CDAFA), Cal. Penal Code § 502 et seq. | Knowingly accessed; and | <u>Common.</u> Whether Google knowingly accessed the Plaintiffs' private browsing information is common to all class members. |
| | Without permission; | <u>Common.</u> That Google did this without providing notice or seeking permission is a common question and Google has not provided any information showing that they did this on an individual basis. |
| | (a)(i) Took, copied, or made use of (ii) any data from a computer, computer system, or computer network; or (b)(i) took or copied (ii) any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network. | <u>Common.</u> How Google collected, stored, and made use of the Plaintiffs' private browsing information is common amongst all class members and proven through expert testimony by Mr. Hochman. |

| | | |
|---|---|---|
| Count Four: Invasion of Privacy | Plaintiffs possessed a legally protected privacy interest; | <u>Common.</u> Whether or not Plaintiffs had a legally protected privacy interest in their private browsing data while in a private browsing mode, is applied class-wide. |
| | Plaintiffs had a reasonable expectation of privacy; and | <u>Common.</u> Whether Plaintiffs had a reasonable expectation of privacy is based on an objective standard, and not an individualized subjective standard. Thus, the same standard will apply to all class members. |
| | Google's intrusion upon that privacy was highly offensive. | <u>Common.</u> Whether Google's invasions on Plaintiffs' privacy is highly offensive turns on whether Google's invasions are: (1) highly offensive to an objectively reasonable person and (2) unacceptable as a matter of public policy. Both questions apply uniformly to all class members. |
| Count Five: Intrusion upon Seclusion | Google intentionally intruded into a private place, conversation, or matter as to which the Plaintiffs had a reasonable expectation of privacy; and | <u>Common.</u> Whether Plaintiffs had a reasonable expectation of seclusion is based on an objective standard, and not an individualized subjective standard. Thus, the same standard will apply to all class members. |
| | Google's occurred in a manner highly offensive to the reasonable person. | <u>Common.</u> Whether Google's intrusions on Plaintiffs' right to seclusion is highly offensive turns on whether Google's intrusions are: (1) highly offensive to an objectively reasonable person and (2) unacceptable as a matter of public policy. Both questions apply uniformly to all class members. |

| | | |
|--|--|---|
| Count Six: Breach of Contract | The existence of a contract; | <u>Common.</u> What contracts are at issue (Google's form contracts and Incognito Mode splash page) is common amongst class members. The meaning of these contracts is based on an objective reading of the contract from the perspective of a reasonable user, not based on an individual Plaintiff's understanding. |
| | Plaintiffs' performance or excuse for non-performance of the contract; | <u>Common.</u> How Plaintiffs performed as Google account users and in using private browsing modes is common amongst class members through the two separate classes. |
| | Google's breach of the contract; and | <u>Common.</u> How Google breached the contract is common amongst all class members. The basis for breach--Google's collection of Plaintiffs' browsing data while in private browsing modes through the use of Google's tracking beacons--is common among class members. |
| | Resulting damage. | <u>Common.</u> Determining the damages that resulting from Google's breach can be modeled and applied on a class-wide basis using common evidence, including Google's own documents describing what Google paid people to allow Google to track their browsing activity. |
| Count Seven: Unfair Competition Law Claim | Google engaged in an unlawful or unfair business act or practice. | <u>Common.</u> Whether Google engaged in an unlawful business practice turns on whether Google violated the laws discussed in the previous claims, which turn on common questions of law and fact. Whether Google engaged in an unfair business practice is common among class members because Google's contracts, statements, and collection of browsing information was executed uniformly amongst all class members. |

APPENDIX B**Exemplar Exhibit List**

This exemplar exhibit list contains as examples exhibits selected from the documents produced by Google. Plaintiffs anticipate that descriptions in the final trial exhibit list would include fewer details. Plaintiffs include these descriptions at this stage to identify key portions from these Google-produced documents. Google stipulated to the authenticity of all of the documents included in this exhibit list (Dkt. 472) but has not yet stipulated to admissibility. To streamline the presentation of evidence at trial, Plaintiffs intend to seek a stipulation from Google to admit these and other Google-produced documents. All of the documents summarized below are attached to the Mao Declaration, concurrently filed with Plaintiffs' motion for class certification.

| No. | Description | Sponsoring Witness | Stipulation to Admit | Objection | Date Admitted |
|-----|---|--|----------------------|-----------|---------------|
| 1 | 2014 Google email criticizing public statement by Google's Eric Schmidt regarding Incognito, stating "people don't and indeed cannot understand Incognito's guarantee(s)" (Mao Decl. Ex. 6 at -75, GOOG-CABR-05287675) | Chris Palmer (deposed Google employee) | | | |
| 2 | 2014 Google email recommending changes to Incognito so "we don't deceive users" (Mao Decl. Ex. 43 at -55, GOOG-BRWN-00457255) | Chris Palmer (deposed Google employee) | | | |
| 3 | 2015 Google internal presentation regarding Incognito "misconceptions" noting "concern about Google collecting data in Incognito" (Mao Decl. Ex. 55 at -14, GOOG-BRWN-00477510) | Adrienne Porter Felt (deposed Google employee) | | | |
| 4 | 2015 Google email describing Incognito as "radioactive" and "effectively a lie" (Mao Decl. Ex. 2 at -26, GOOG-BRWN-00806426) | Chris Palmer (deposed Google employee) | | | |
| 5 | 2015 Google email discussing Incognito "problem" and how "the fault lies partly with the name and the iconography" used by Google (Mao Decl. Ex. 65 at -79, GOOG-CABR-05370279) | Chris Palmer (deposed Google employee) | | | |
| 6 | 2016 Google email discussing how Google was "struggling with the Incognito branding and misconceptions it causes" (Mao Decl. Ex. 66 at -18, GOOG-BRWN-00390418) | Sabine Borsay (to be deposed Google employee) | | | |
| 7 | 2016 Google email discussing Incognito and how "[t]his is a problem of professional ethics and basic honesty" (Mao Decl. Ex. 7 at -04, GOOG-CABR-04971904) | Chris Palmer (deposed Google employee) | | | |
| 8 | 2016 Google email discussing Incognito and how "nothing will be more scannable than the name and icon, both of which are a poor fit for what the feature actually provides" (Mao Decl. Ex. 67 at -84, GOOG-BRWN-00410884) | Chris Palmer (deposed Google employee) | | | |

| | | | | | |
|----|---|--|--|--|--|
| 9 | 2018 Google email stating “the ‘incognito’ war was waged and lost years ago” and that Incognito “has always been a misleading name” (Mao Decl. Ex. 4 at -63, GOOG-BRWN-00475063) | Chris Palmer (deposed Google employee) | | | |
| 10 | 2018 Google internal document titled “Five ways people misunderstand Incognito and private browsing” noting “common misconceptions” that could give a “false impression of privacy” (Mao Decl. Ex. 68 at -52, GOOG-CABR-04718352) | Martin Shelton (deposed former Google employee) | | | |
| 11 | 2018 Google internal presentation titled “The Incognito Problem” noting Google branding and disclosures “confuse people” with Google “over-promising and under-delivering” (Mao Decl. Ex. 12 at -98, -302, GOOG-BRWN-00140297) | Chris Palmer (deposed Google employee) | | | |
| 12 | 2018 Google email agreeing “there is an incognito problem” (Mao Decl. Ex. 69 at -12, GOOG-BRWN-00804212) | Adrienne Porter Felt (deposed Google employee) | | | |
| 13 | 2018 Google email discussing how words “Incognito” and “private” reinforce “misperception that your browsing is private everywhere instead of just on your device” (Mao Decl. Ex. 70 at -49, GOOG-CABR-03764749) | Martin Shelton (deposed former Google employee) | | | |
| 14 | 2018 Google internal document noting Incognito “spy icon may be misleading” and discussing how to “rebrand incognito and set the user expectation correctly” (Mao Decl. Ex. 46 at -97, GOOG-BRWN-00047390) | Ramin Halavati (deposed Google employee) | | | |
| 15 | 2018 Google email stating “misconceptions flow directly from the framing of the feature as ‘Incognito’ (or, for other browsers, ‘Private’)” (Mao Decl. Ex. 71 at -80, GOOG-CABR-04261880) | Chris Palmer (deposed Google employee) | | | |

| | | | | | |
|----|--|--|--|--|--|
| 16 | 2018 Google email stating “the blame for people’s misconceptions about Incognito Mode is due to that name and branding” as “argued repeatedly” (Mao Decl. Ex. 72 at -81, GOOG-CABR-03923580) | Chris Palmer (deposed Google employee) | | | |
| 17 | 2018 Google email stating “incognito is a confusing mess” (Mao Decl. Ex. 73 at -63, GOOG-CABR-03827263) | Adrienne Porter Felt (deposed Google employee) | | | |
| 18 | 2018 Google internal document noting “gap between our promises about Chrome Incognito mode, their delivery, and user expectations” (Mao Decl. Ex. 74 at -99, GOOG-BRWN-00047399) | Ramin Halavati (deposed Google employee) | | | |
| 19 | 2019 Google internal document regarding Incognito stating “most users do not correctly understand the current messaging” and need to clarify whether users are “protected from Google” (Mao Decl. Ex. 52 at -50, GOOG-CABR-00094550) | Rory McClelland (deposed former Google employee) | | | |
| 20 | 2019 Google email noting upcoming review with CEO Sundar Pichai to discuss “[e]nhancements to Incognito, in line with the thinking from Chris Palmer and others” (Mao Decl. Ex. 75 at -31, GOOG-CABR-04991831) | AbdelKarim Mardini (deposed Google employee) | | | |
| 21 | 2019 Google internal document for CEO Sundar Pichai instructing him to not use the word “private” to describe Incognito due to “known misconceptions” (Mao Decl. Ex. 20 at -68.C, GOOG-BRWN-00048967.C) | AbdelKarim Mardini (deposed Google employee) | | | |
| 22 | 2019 Google email stating CEO “Sundar [Pichai] didn’t want to put incognito under the spotlight” (Mao Decl. Ex. 10 at -93, GOOG-BRWN-00388293) | AbdelKarim Mardini (deposed Google employee) | | | |
| 23 | 2019 Google internal presentation noting Incognito “[u]sers currently believe that none of their data is collected and they are essential [sic] anonymous” (Mao Decl. Ex. 76 at -41, GOOG-BRWN-00047341) | Sabine Borsay (to be deposed Google employee) | | | |

| | | | | | |
|----|--|--|--|--|--|
| 24 | 2019 Google internal presentation for CEO Sundar Pichai noting Chrome “[p]rivacy-related controls are hidden ... overwhelming ... and difficult to understand” (Mao Decl. Ex. 77 at -85, GOOG-CABR-05269678) | AbdelKarim Mardini (deposed Google employee) | | | |
| 25 | 2019 Google internal presentation discussing “simpler way to explain Incognito” including as to whether Google “save[s] personal data” and “IP addresses or other unique IDs” (Mao Decl. Ex. 78 at -55, GOOG-CABR-04798344) | AbdelKarim Mardini (deposed Google employee) | | | |
| 26 | 2020 Google email stating “[c]urrently we are logging all user activities in incognito mode server-side, and that is more or less linkable to users signed-in data” (Mao Decl. Ex. 79 at -91, GOOG-BRWN-00701189) | Ramin Halavati (deposed Google employee) | | | |
| 27 | 2020 Google internal presentation noting private browsing users “do not understand how private mode works” with “several common misconceptions” including that it “hides browsing activity from Google” (Mao Decl. Ex. 80 at -03, GOOG-BRWN-00042388) | Ramin Halavati (deposed Google employee) | | | |
| 28 | 2020 Google internal presentation noting “[u]sers overestimate the protections that Incognito mode provides” with “significant misconceptions about features, security benefits, and data collection” (Mao Decl. Ex. 81 at -13, GOOG-CABR-04431207) | AbdelKarim Mardini (deposed Google employee) | | | |
| 29 | 2020 Google email noting “I’m struggling to come up with any research for Incognito that doesn’t highlight how broken it is” (Mao Decl. Ex. 3 at -85, GOOG-BRWN-00441285) | Sammit Adhya (deposed Google employee) | | | |
| 30 | 2020 Google internal document discussing Incognito and noting “It’s not private in ways that many users want, that is, as to Google” and “you don’t have the ability to see or delete” data, “Google has it” (Mao Decl. Ex. 85 at -56.C, GOOG-BRWN-00153850.C) | Greg Fair (deposed Google employee) | | | |

| | | | | | |
|----|--|---|--|--|--|
| 31 | 2021 Google email to CEO Sundar Pichai characterizing Incognito as “not truly private” (Mao Decl. Ex. 1 at -67, GOOG-BRWN-00406065) | Lorraine Twohill (deposed Google employee) | | | |
| 32 | 2021 Google internal presentation noting Incognito “[u]sers overestimate the protections that Incognito provides and are unaware of the personalization and data collection that occurs” (Mao Decl. Ex. 82 at -50, GOOG-CABR-04738550) | AbdelKarim Mardini (deposed Google employee) | | | |
| 33 | 2021 Google internal document proposing changes to Incognito disclosures to “clear up known user misconceptions” (Mao Decl. Ex. 83 at -41, GOOG-CABR-04739841) | Ramin Halavati (deposed Google employee) | | | |
| 34 | 2021 Google email noting “[u]sers have misconceptions about Incognito and often overestimate the protections available” (Mao Decl. Ex. 49 at -51, GOOG-CABR-04668451) | AbdelKarim Mardini (deposed Google employee) | | | |
| 35 | 2021 Google internal presentation proposing to remove “Now you can browse privately” from Incognito screen because “the word ‘private’” poses “the risk of overestimating the protection Incognito offers” (Mao Decl. Ex. 84 at -72, GOOG-CABR-04746153) | Sabine Borsay (to be deposed Google employee) | | | |